(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

**特開平6－204998**

(43)公開日　平成６年(1994)７月22日

| (51)Int.Cl.[5] | 識別記号 | 庁内整理番号 | Ｆ Ｉ | 技術表示箇所 |
|---|---|---|---|---|
| Ｈ０４Ｌ　9/00 | | | | |
| 9/10 | | | | |
| 9/12 | | | | |
| | | 7117－5K | Ｈ０４Ｌ　9/ 00 | Ｚ |
| | | 8732－5K | 11/ 26 | |

審査請求　未請求　請求項の数19(全 12 頁)　最終頁に続く

(21)出願番号　特願平5－237161

(22)出願日　平成５年(1993)８月31日

(31)優先権主張番号　９３７００９

(32)優先日　1992年８月31日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390035493
アメリカン　テレフォン　アンド　テレグラフ　カムパニー
AMERICAN TELEPHONE AND TELEGPAPH COMPANY
アメリカ合衆国　10013－2412　ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　32

(74)代理人　弁理士　三俣　弘文

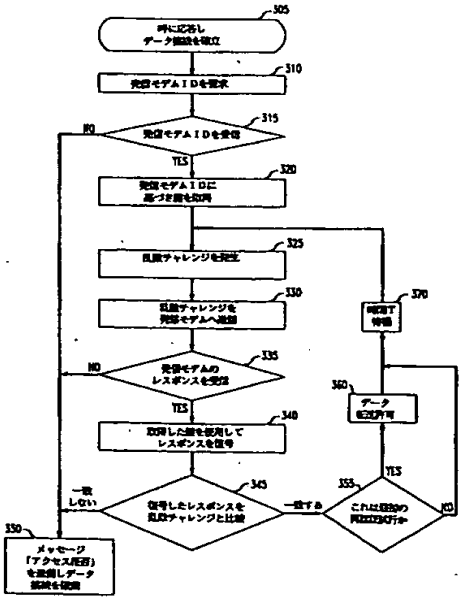
最終頁に続く

(54)【発明の名称】　データ通信装置およびデータ通信方法

(57)【要約】

【目的】　コンピュータ設備とユーザの間の公衆交換電話網（ＰＳＴＮ）のモデム間の再認証手続きによって、侵入者によるアクティブ傍受に対してコンピュータ設備を保護する安全な方法を提供する。

【構成】　ユーザのモデムとコンピュータのモデムは、データ接続期間中再認証手続きを実行する。この再認証手続きはデータ接続のサイドチャネルで透過的に実行される。このサイドチャネルは帯域内チャネルでも帯域外チャネルでもよい。再認証手続きは、２つのモデム間での暗号化された情報の交換からなる。一方のモデムがアクティブ傍受の存在を検出すると、モデムは単にデータ接続を中断する。



1

【特許請求の範囲】

【請求項１】　他のデータ通信装置へ複数のチャレンジを送信し、そのデータ通信装置からその複数のチャレンジのそれぞれに対応する複数のレスポンスを受信する送受信手段と、

各レスポンスの確認を表す出力を生成するために、各チャレンジの関数として各レスポンスを確認する手段とからなり、

その確認によって、出力が、レスポンスのうちの１つが確認されないことを表している場合にデータ接続を中断することを特徴とする、データ接続のユーザを再認証するデータ通信装置。

【請求項２】　前記確認手段が、前記他のデータ通信装置の識別子の関数でもあることを特徴とする請求項１の装置。

【請求項３】　前記送受信手段が、前記他のデータ通信装置に識別情報の要求を送信し、前記他のデータ通信装置からその識別子を受信することを特徴とする請求項２の装置。

【請求項４】　前記確認手段が複数の復号されたレスポンスを生成し、そのそれぞれは、前記他のデータ通信装置の識別子の関数として選択されたデータ暗号化鍵の関数であり、前記確認手段が、復号された各レスポンスを、各チャレンジと比較して確認を表す出力を生成し、それによって、チャレンジと、復号されたレスポンスの間に不一致がある場合にデータ接続を中断することを特徴とする請求項３の装置。

【請求項５】　前記確認手段が各チャレンジを暗号化し、その暗号化は、前記他のデータ通信装置の識別子の関数として選択されたデータ暗号化鍵の関数であり、前記確認手段が、各レスポンスを、暗号化された各チャレンジと比較して確認を表す出力を生成し、それによって、暗号化されたチャレンジとレスポンスの間に不一致がある場合にデータ接続を中断することを特徴とする請求項３の装置。

【請求項６】　前記確認手段が対称データ暗号化アルゴリズムの関数であることを特徴とする請求項１の装置。

【請求項７】　前記確認手段が非対称データ暗号化アルゴリズムの関数であることを特徴とする請求項１の装置。

【請求項８】　各チャレンジが乱数であり、前記データ通信装置がモデムであることを特徴とする請求項１の装置。

【請求項９】　第１のデータ通信装置とユーザの第２のデータ通信装置からなるデータ接続において、第１データ通信装置で使用するための、ユーザを再認証するデータ通信方法において、

第２データ通信装置へ複数のチャレンジを送信し、そのデータ通信装置からその複数のチャレンジのそれぞれに対応する複数のレスポンスを受信する送受信ステップと、

各レスポンスの確認を表す出力を生成するために、各チャレンジの関数として各レスポンスを確認するステップとからなり、

その確認によって、出力が、レスポンスのうちの１つが確認されないことを表している場合にデータ接続を中断することを特徴とする、データ通信方法。

【請求項１０】　前記確認ステップが、第２データ通信装置の識別子の関数でもあることを特徴とする請求項９の方法。

【請求項１１】　前記送受信ステップが、第２データ通信装置に識別情報の要求を送信し、第２データ通信装置からその識別子を受信することを特徴とする請求項１０の方法。

【請求項１２】　前記確認ステップが、

それぞれ、第２データ通信装置の識別子の関数として選択されたデータ暗号化鍵の関数である複数の復号されたレスポンスを生成するステップと、

確認を表す出力を生成するために、復号された各レスポンスを各チャレンジと比較するステップとを有し、その比較によって、チャレンジと復号されたレスポンスの間に不一致がある場合にデータ接続を中断することを特徴とする請求項１１の方法。

【請求項１３】　前記確認ステップが、

第２データ通信装置の識別子の関数として選択されたデータ暗号化鍵の関数として各チャレンジを暗号化するステップと、

確認を表す出力を生成するために、各レスポンスを、暗号化された各チャレンジと比較するステップとを有し、その比較によって、暗号化されたチャレンジとレスポンスの間に不一致がある場合にデータ接続を中断することを特徴とする請求項１１の方法。

【請求項１４】　前記確認ステップが対称データ暗号化アルゴリズムの関数であることを特徴とする請求項９の方法。

【請求項１５】　前記確認ステップが非対称データ暗号化アルゴリズムの関数であることを特徴とする請求項９の方法。

【請求項１６】　各チャレンジが乱数であり、データ通信装置がモデムであることを特徴とする請求項９の方法。

【請求項１７】　第１のデータ通信装置とユーザの第２のデータ通信装置からなるデータ接続においてユーザを再認証するデータ通信方法において、

ａ）それぞれデータ暗号化鍵に関係づけられた複数の識別番号からなる鍵リストを第１データ通信装置に格納するステップと、

ｂ）第１データ通信装置において第２データ通信装置から識別番号を受信するステップと、

ｃ）第２データ通信装置から受信した識別番号に関係づ

けられたデータ暗号化鍵を鍵リストから取得するステップと、

ｄ）第１データ通信装置から第２データ通信装置へ、番号からなるチャレンジを送信するステップと、

ｅ）第１データ通信装置において第２データ通信装置から、番号からなるレスポンスを受信するステップと、

ｆ）第１データ通信装置において、レスポンスの確認を表す出力を生成するために、第２データ通信装置からのレスポンスを、取得したデータ暗号化鍵の関数として処理し、その出力が、第２データ通信装置の識別子の確認を表している場合にステップｄ）からｆ）までを反復し、第２データ通信装置の識別子が確認されなかった場合にデータ接続を中断するステップとからなることを特徴とするデータ通信方法。

【請求項１８】　ステップｆ）が、

復号されたレスポンスを生成するために、取得したデータ暗号化鍵の関数としてレスポンスを復号することによって第２データ通信装置からのレスポンスを処理するステップと、

復号されたレスポンスをステップｄ）のチャレンジと比較し、復号されたレスポンスがステップｄ）のチャレンジと等しい場合にステップｄ）からｆ）までを反復し、復号されたレスポンスがステップｄ）のチャレンジに等しくない場合にデータ接続を中断するステップとを有することを特徴とする請求項１７の方法。

【請求項１９】　ステップｆ）が、

暗号化されたチャレンジを生成するために、取得したデータ暗号化鍵の関数としてチャレンジを暗号化することによって第２データ通信装置からのレスポンスを処理するステップと、

レスポンスを暗号化されたチャレンジと比較し、レスポンスが暗号化されたチャレンジに等しい場合にステップｄ）からｆ）までを反復し、レスポンスが暗号化されたチャレンジに等しくない場合にデータ接続を中断するステップとを有することを特徴とする請求項１７の方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、モデムおよびコンピュータシステムに関する。特に、本発明は、コンピュータシステムへの安全なアクセスを提供するモデムの使用に関する。

【０００２】

【従来の技術】今日の世界におけるコンピュータの使用は、メインフレームからパーソナルコンピュータに至るまで、連続的に増加しており、ますます多くの人々がコンピュータシステムを使用しつつある。実際、コンピュータ自体へのアクセスが可能であることによって、ほとんどの人が、モデムおよび公衆交換電話網（ＰＳＴＮ）を通じて、コンピュータの使用から恩恵を受けることが可能になっている。残念ながら、このアクセス可能性



は、「侵入者」、すなわち、コンピュータシステムの違法ユーザを引き付けているようにも思われる。その結果、コンピュータに格納されている情報の正当性および分配に関する、コンピュータシステム、またさらにはコンピュータの網のセキュリティは、コンピュータの合法ユーザ、所有者、およびオペレータの関心の事項となっている。

【０００３】ある種のアクセスセキュリティをコンピュータシステムに提供するこの必要性に応答して、アクセス要求ユーザの同一性を認証するためにさまざまな方法が使用されている。１つの例は、周知のとおり、「パスワード」の使用である。この変形として、モデムアクセスの場合、「パスワード／コールバック」方式がある。これは、ユーザによるパスワードの入力が成功した後、被呼コンピュータが所定の電話番号でユーザにコールバックするものである。もう１つの例は、チャレンジ／レスポンス方式である。これは、コンピュータ（付与者）が、乱数（チャレンジ）をユーザ（要求者）へ送信し、要求者は、付与者と要求者によって共有されている秘密の鍵（キー）を使用してその乱数を暗号化することによって、要求者の同一性を証明する、というものである。実際、「チャレンジ／レスポンス」プロトコルおよびデータ暗号化規格（ＤＥＳ）アルゴリズムを使用した強力なノード間認証手続きを提供する、ＡＮＳＩ　Ｘ９．２６－１９９０「卸売財務システム用開始認証」のような工業規格がある。

【０００４】しかし、パスワードおよびパスワード／コールバック方式は、後でデータ接続を制御し、それによってコンピュータシステムを「欺く」者に対する保護を提供することはほとんどできない。さらに、ＡＮＳＩ　Ｘ９．２６－１９９０のチャレンジ／レスポンス法は、最初の開始（ログイン）手続き中にユーザの同一性を認証する方法を与えるのみである。換言すれば、上記の方法は、最初の開始手続き後にユーザを切断し、コンピュータにアクセスするためのデータ接続の侵入者による制御を可能にする「アクティブ傍受」を使用する侵入者に対する保護はしない。

【０００５】その結果、コンピュータシステムへのアクセスセキュリティが、データ接続自体のプライバシーと比べて最重要事項である場合、データ接続がアクティブ傍受に侵されないことを保証する他の技術が要求される。例えば、ＤＥＳ暗号化を使用したデータストリームの完全な暗号化は、侵入者が後でアクセスすることを防ぐ１つの可能な手段である。もう１つの手段が、米国特許第４，８０２，２１７号（発明者：ミチェナー（Ｍｉｃｈｅｎｅｒ）、発行日：１９８９年１月３１日）に記載されている。それによれば、コンピュータが、ユーザの端末とユーザのモデムの間に接続されたセキュリティデバイスを制御する。特に、ユーザは、コンピュータシステムにダイヤルし、コンピュータシステムはセキュリ

ティデバイスから暗号化された第１の符号語を受信する。続いて、コンピュータは、セキュリティデバイスに対し、この第１暗号化符号語を第２の暗号化された符号語に変更するよう命令し、ラインを切断し、ユーザにコールバックする。コンピュータによるコールバックが完了すると、セキュリティデバイスは、データ接続を確立するために、第２暗号化符号語をコンピュータに送信する。その後、コンピュータは、セキュリティデバイスに対し、定期的に、他の暗号化符号語に変更するよう命令し、そのたびに、セキュリティデバイスは、新たに暗号化された符号語をコンピュータに送信し、それに対してコンピュータは受信した暗号化符号語をチェックし、それによって、もとのユーザへのデータ接続の正当性の継続を確認する。

【０００６】

【発明が解決しようとする課題】結果として、完全なデータ暗号化によって、または、ミチェナー特許によって提案されたように、定期的再認証によって、同一性の一定の再確認がなければ、侵入者はラインを橋絡し、データ接続を引き継ぎ、それによって、リソースおよび情報への無許可のアクセスを取得し、有利になるように情報を注入することができる。しかし、この従来技術は、アクティブ傍受に対するあるレベルの保護は提供するが、問題に対する完全な解答ではない。例えば、完全なデータ暗号化は、一般にコンピュータおよびユーザの端末に関して、コンピュータシステムのコストおよび複雑さの両方に影響する。同様に、ミチェナー特許は、コンピュータソフトウェアの修正、および、ユーザの端末とユーザのモデムの間の別個のセキュリティデバイスを必要とする。

【０００７】

【課題を解決するための手段】本発明は、コンピュータのユーザ、所有者、およびオペレータに、コンピュータへのＰＳＴＮデータ接続のアクティブ傍受に対するアクセスセキュリティを提供する際の柔軟性を提供する。特に、われわれの認識では、ＰＳＴＮデータ接続において一般的に共通の要素の１つは、端末機器と伝送媒体の間を媒介する機器、すなわち、モデムである。従って、本発明の原理によれば、モデム間の連続的再認証手続きによってアクセスセキュリティがＰＳＴＮデータ接続に与えられる。この連続的再認証手続きは、データ接続期間中に認証情報を定期的または非定期的に送信するために、データ接続のサイドチャネルを使用することによって、非干渉的に行われる。このサイドチャネルは、帯域内でもよい。この場合、再認証情報はデータ伝送間に時分割多重化される。または、サイドチャネルは帯域外でもよい。この場合、利用可能帯域幅の狭い部分が、周波数分割多重（ＦＤＭ）方式を使用して再認証情報を交換するために使用される。その結果、アクセスセキュリティがＰＳＴＮデータ接続に透過的に提供され、追加のセキュリティデバイスやユーザの機器またはコンピュータシステムへの修正は不要となる。

【０００８】本発明の一実施例では、着信モデムおよび発信モデムの両方がＤＥＳアルゴリズムをサポートし、着信モデムは発信モデムを再認証する。発信モデムを再認証するため、着信モデムは、データ接続期間中ときどきチャレンジ／レスポンスシーケンスを発信する。特に、着信モデムは、データ暗号化鍵のリストを有し、各データ暗号化鍵は、特定モデムの識別子に対応する。電話呼に応答すると、着信モデムは、発信モデムに対し、対応するデータ暗号化鍵を選択することができるように、識別子を送信することによって、自分自身を識別するよう要求する。その後、着信モデムは、ときどき、発信モデムにチャレンジとして送信される乱数を発生する。発信モデムは、チャレンジを受信すると、着信モデムにレスポンスを返す。このレスポンスは、乱数の暗号化された形式である。発信モデムの暗号化プロセスは、着信モデムによって使用されたデータ暗号化鍵と同一のデータ暗号化鍵を使用する。着信モデムは、そのレスポンスを復号し、それをチャレンジと比較する。復号したレスポンスとチャレンジが一致した場合、発信モデムの同一性が確認される。しかし、復号したレスポンスとチャレンジが一致しない場合、詐欺の可能性のある試行が検出されたことを示し、着信モデムはデータ接続を単に破棄する。

【０００９】

【実施例】図１に、二地点間データ通信システムを示す。以下の例では、端末１１０の発呼者（ユーザ）が、発信モデム１２０、電話網１３０、および着信モデム２００を通じて被呼者（コンピュータ１５０）にアクセスするために、電話呼を発信すると仮定する。ライン２０１および１２１は、電話網１３０によって提供される一般的な「チップ／リング」、すなわちローカルループのアクセスを表す。モデム１２０および２００の両方が本発明の原理を実現するが、簡単のためモデム２００のみ詳細を図２に示す。以下で説明する本発明の概念を除いて、モデム２００は、従来周知のデータ通信機器（ＤＣＥ）を表し、データ端末機器（例えばコンピュータ１５０）とデータ回線（ここではＰＳＴＮ）をインタフェースする。ＰＳＴＮはライン２０１および１２１、ならびに電話網１３０によって表される。特に、本発明の説明では、データ通信機器という用語は、１）データ接続を確立するのに必要な機能、ならびに２）データ端末機器とデータ回線の間の信号変換および符号化を提供する装置を意味する。モデム２００は、メモリ２２０、ＣＰＵ２１０、ディジタル信号プロセッサ（ＤＳＰ）２５０、データ暗号化プロセッサ２３０、データ通信インタフェース２６０、およびデータ端末インタフェース２４０からなる。ＣＰＵ２１０はマイクロプロセッサ中央処理装置であり、バス２１１を通じてメモリ２２０に格納され

たプログラムデータに作用し、またはそれを実行する。メモリ２２０はランダムアクセスメモリを表し、いくつかの代表的な記憶ロケーションを有し、そのサブセットが図２に示されている。メモリ２２０は、鍵リスト２２１を有すると仮定する。データ暗号化プロセッサ２３０はＤＥＳ暗号化規格をサポートし、リード２１３を通じてＣＰＵ２１０によって供給されるデータに作用する。例えば、データ暗号化プロセッサ２３０は、ＤＥＳ規格（例えば「連邦情報処理規格４６」）によって指定される「電子コードブック暗号化」プロセスに従って作用する。注意すべきことであるが、明確化のため、データ暗号化プロセッサ２３０はＣＰＵ２１０およびメモリ２２０とは別に図示されている。しかし、以下の説明から明らかになるように、もう１つの、より安価な実現は、データ暗号化プロセッサ２３０によって実行されるデータ暗号化アルゴリズムが単にＣＰＵ２１０によって直接実行され、その場合ＣＰＵ２１０はメモリ２２０に格納されたデータ暗号化プログラムを実行するというものである。最後に、簡単のため、ＤＳＰ２５０は、入力または出力信号を処理するための、フィルタ、アナログーディジタル変換器およびディジタルーアナログ変換器のような他の周知の処理機能を有すると仮定する。

【００１０】モデム１２０からの発信電話呼の結果、モデム２００は電話網１３０からリード２０１によって入力信号を受信する。この入力信号は、データ通信インタフェース２６０によってＤＳＰ２５０に送られる。ＤＳＰ２５０は、ＣＰＵ２１０の制御下で、ＣＣＩＴＴ Ｖ．３２呼確立シーケンスを実行する。このシーケンスは、モデム１２０とのデータ接続を確立するためのモデムハンドシェイクおよびトレーニングを含む。データ接続の確立後、ＤＳＰ２５０は、コンピュータ１５０（データ端末インタフェース２４０を通じて）と端末１１０（データ通信インタフェース２６０を通じて）との間で生じるデータストリームの信号変換および符号化を実行する。

【００１１】本発明の原理によれば、着信モデム２００は、チャレンジ／レスポンスプロトコルによって、発信モデム１２０のユーザ透過的（暗号）一方向ノード間再認証を実行する。その流れ図を図３に示す。特に、ステップ３０５で、発信モデム１２０とのデータ接続を確立した後、ＣＰＵ２１０はステップ３１０に進み、ＤＳＰ２５０を通じてモデム識別（ＩＤ）番号をモデム１２０に要求する。モデムＩＤ番号とは、発信モデムに割り当てられた所定の番号である（後述）。ステップ３１５で、ＣＰＵ２１０が、発信モデムのＩＤ番号を受信しない場合、ステップ３５０で、ＣＰＵ２１０は単にメッセージ「アクセス拒否」を送信し、データ接続を破棄する。一方、ＣＰＵ２１０が発信モデムのＩＤ番号を受信した場合、ＣＰＵ２１０はステップ３２０に進み、鍵リスト２２１から対応するデータ暗号化鍵を取得する。鍵リスト２２１は、事前にメモリ２２０に格納されており、複数のモデムＩＤ番号を表す。各モデムＩＤ番号はそれぞれ可能な発信モデムを表し、データ暗号化鍵に関係づけられている。この関係づけられたデータ暗号化鍵もまた、モデムＩＤと同様に、発信モデムにおいて事前に決定されている。

【００１２】モデム１２０のデータ暗号化鍵を取得した後、ステップ３２５で、ＣＰＵ２１０は乱数を発生する。これはチャレンジとして知られる。ステップ３３０で、このチャレンジはモデム１２０に送信される。モデムからチャレンジを受信すると、モデム１２０は、データ暗号化プロセッサ（図示せず）によってそのチャレンジを暗号化し、レスポンス（すなわち、ある形式の「暗号文」）を発生し、モデム２００に返送する。モデム１２０によって実行される暗号化は、上記の格納されているデータ暗号化鍵を使用する。チャレンジおよびレスポンスはそれぞれ少なくとも２０ビットのデータからなるため、正しいレスポンスを発見する可能性は１００万分の１しかない。ステップ３３５で、ＣＰＵ２１０がモデム１２０からレスポンスを受信しない場合、ステップ３５０で、ＣＰＵ２１０はメッセージ「アクセス拒否」を送信し、データ接続を破棄する。一方、ＣＰＵ２１０がレスポンスを受信した場合、ＣＰＵ２１０はステップ３４０に進み、ステップ３２０で取得したデータ暗号化鍵を使用してその応答を復号する。受信したレスポンスの復号は、ＤＥＳ暗号化規格をサポートするデータ暗号化プロセッサ２３０を介してＣＰＵ２１０によって実行される。続いてＣＰＵ２１０はモデム１２０の同一性を確認する。ステップ３４５で、復号したレスポンスとチャレンジが一致しない場合、ステップ３５０で、ＣＰＵ２１０はメッセージ「アクセス拒否」を送信し、データ接続を中断（例えば破棄）する。（この時点で、着信モデム２００には別の選択肢があることに注意すべきである。例えば、データ接続を破棄する代わりに、データ接続の「トレース」を開始することができる。）一方、ＣＰＵ２１０が、モデム１２０の同一性を確認した場合、すなわち、復号したレスポンスとチャレンジが一致した場合、ＣＰＵ２１０はデータ接続を妨害せずにステップ３５５に進み、これが最初の再認証試行の完了であるかどうかをチェックする。これが最初の再認証試行の完了である場合、ステップ３６０で、ＣＰＵ２１０は、モデム２００とモデム１２０の間のデータ情報の転送を可能にする。いったんデータ転送が可能となると、後の再認証試行はステップ３６０をバイパスして直接ステップ３７０にすみ、ＣＰＵ２１０は所定時間Ｔの割り込みをセットする。時間Ｔの経過後、ＣＰＵ２１０は、ステップ３２５～３４５を反復することによって、データ接続を再認証する。この再認証プロセスは、データ接続期間中継続される。

【００１３】上記の認証プロセスを図４にも示す。着信

モデム３００（付与者）は、「モデムＩＤ送信」メッセージ６０５を発信モデム１２０（要求者）に送信し、発信モデム１２０は「ＩＤ」６１０を送信することによって応答する。その後、着信モデム２００は「チャレンジ」６１５を発信モデム１２０に送信し、発信モデム１２０は、「レスポンス」６２０を送信する。レスポンス６２０の復号が、上記のように、チャレンジ６１５と一致した場合、着信モデム２００は「ＯＫ」メッセージ６２５を送信することができる。一方、レスポンス６２０の復号がチャレンジ６１５と一致しない場合、モデム２００は「アクセス拒否」メッセージ６３０を送信する。

【００１４】上記の図３以外のもう１つの方法を図５に示す。相違点はステップ５４０および５４５のみである。ステップ５４０で、モデム２００は、ステップ３３０でモデム１２０に送信したチャレンジを暗号化する。このチャレンジは、ステップ３２０で取得したモデム１２０に関係づけられたデータ暗号化鍵を使用して暗号化される。モデム１２０の同一性の確認は、ステップ５４５で、暗号化したチャレンジとモデム１２０からのレスポンスとを比較することによって実行される。上記のように、モデム１２０によって暗号化されたチャレンジ（すなわち、レスポンス）が、モデム２００によって暗号化されたチャレンジと一致した場合、データ接続は妨害されず、ＣＰＵ２１０はステップ３５５に進む。しかし、一致しない場合、ステップ３５０で、データ接続は中断される。

【００１５】上記の図３および５の再認証プロセスは、データ接続のサイドチャネルで実行される。換言すれば、データ接続の帯域幅の一部が再認証情報を伝送するために使用される。その結果、データ接続は、基本チャネル（データ伝送用）およびサイドチャネル（補助的情報伝送用）からなる。このサイドチャネルは、基本的に、再認証情報をデータの伝送と多重化する。特に、サイドチャネルでは、帯域内チャネルまたは帯域外チャネルが使用される。

【００１６】帯域外サイドチャネルの例は、データと再認証情報の周波数分割多重化（ＦＤＭ）をするものである。この形式の帯域外チャネルは「二次チャネル」としても知られており、一般的に、低ビットレートチャネル専用の、周波数スペクトルの狭い部分である。周波数スペクトルの例を図６に示す。データ接続は、帯域幅$f_w$を有し、データ情報を伝送する基本チャネル４１０と、帯域幅$f_n$を有し、再認証情報を伝送する補助（狭帯域）チャネル４０５からなると仮定している。

【００１７】帯域内サイドチャネルの例は、データと再認証情報の時分割多重化をするものである。これを図７に示す。モデム２００とモデム１２０間でのデータの伝送の実際の構造は、下位のモデムプロトコル（例えばＣＣＩＴＴ　Ｖ．４２の改訂版）を利用すると仮定する。このプロトコルは、データの伝送用の「データフレーム」と、制御（補助）情報の伝送用の「制御フレーム」とからなるＨＤＬＣ型のプロトコルである。図７に示すように、データフレーム（例えばデータフレーム５１０）は、制御フレーム（例えば制御フレーム５０５）と時分割多重化されている。再認証情報は、制御フレーム５０５内で周知技術を使用してモデム２００と１２０の間で単に伝送される。

【００１８】上記のように、発信モデムと着信モデムは、再認証プロセス中、同一のデータ暗号化鍵を共有する。これは、「対称」データ暗号化として知られている。結果として、両方のモデムは同一のデータ暗号化鍵情報を格納していなければならない。さらに、少なくとも発信モデムはそのモデムＩＤを格納していなければならない。最後に、一方または両方のモデムは、上記の鍵リストを保持する。このリストは、可能な発信モデムＩＤのリストを、識別されるモデムに格納されているデータ暗号化鍵と同一のデータ暗号化鍵にそれぞれ関係づける。これらの情報はすべて、モデムパラメータの管理のための従来技術を使用して事前に初期化される。例えば、この情報は、モデムに接続された端末を通じて入力することも、「ダウンロード」方式を使用することによって遠隔で初期化することも可能である。

【００１９】上記の反復再認証プロトコルは、チャレンジ／レスポンスプロトコルを例示しているが、他の再認証プロトコルも可能である。例えば、上記の方法よりは安全ではないが、モデム１２０および２００は単純なパスワード方式を使用することができる。この場合、各モデムは同一のパスワードのリストを有し、各パスワードには番号が関係づけられる。この方式では、モデム２００によって送信されるチャレンジは単にパスワードに関係づけられた番号である。モデム１２０によるレスポンスは単にその番号（チャレンジ）に割り当てられたパスワードである。モデム２００は、モデム１２０の認証を判定するために、受信したパスワード（レスポンス）を、パスワードのリストに示された正確なパスワードと比較する。

【００２０】もう１つの例は、上記の対称データ暗号化チャレンジ／レスポンスプロトコルと同様に安全なものであるが、「公開鍵」方式の使用である。これは、米国規格技術協会（ＮＩＳＴ）によって開発され現在提案されている「ディジタル署名規格」のような「非対称」形式のデータ暗号化である。公開鍵方式は、暗号化と復号に異なる鍵が使用されるため、非対称である。さらに、一方の鍵は秘密に保持される。他方の鍵は公開してよい。特に、モデム２００は、上記のように、モデム１２０へチャレンジを送信する。しかし、モデム１２０は、「ディジタル署名」および「証明書」を添付してそのチャレンジを返す。ディジタル署名とは、チャレンジおよびモデム１２０の秘密のデータ暗号化鍵の関数であるディジタルビットパターンであって、モデム２００には未

知である。証明書は、周知のように、モデム１２０からの識別情報および公開鍵を含む。この方法では、「要求者」が常に公開鍵を提供するため、モデム２００はモデム識別子およびデータ暗号化鍵のリストを保持する必要はない。

【００２１】以上、本発明の実施例を説明したが、本発明の原理に基づいてさまざまな変形例が可能である。例えば、上記の連続的再認証プロセスはモデム間データ接続に関して説明したが、他の形式のデータ通信機器（例えば端末アダプタ）もこの連続的再認証を実行することが可能である。

【００２２】さらに、再認証は連続的であるが、再認証試行間の時間遅延Ｔは周期的である必要はなく、データ接続期間中「非周期的」、すなわち可変とすることが可能である。さらに、他の形式のサイドチャネル（例えば、基本信号点コンステレーションの変調）が可能である。また、上記では発信モデムのＩＤはハンドシェイクプロセスの後に受信したが、モデム識別情報の受信はハンドシェイクプロセス中に行うことも可能である。

【００２３】また、上記の例では、暗号化を使用した一方向チャレンジ／レスポンス認証について説明したが、任意の種類の認証プロトコル（例えば、双方向のノード間再認証プロトコル）が、通信エンティティの識別子を認証するために使用可能である。例えば、双方向再認証プロトコルを実現するには、発信モデムは上記（図３）の着信モデムと同様のステップを実行する。特に、発信モデムもまた、着信モデムに自分自身を識別するよう要求し、その後、発信モデムは、着信モデムによって正確に暗号化されなければならないチャレンジを発行する。着信モデムの復号されたレスポンスが発信モデムのチャレンジと一致しない場合、発信モデムはデータ接続を中断する。

【００２４】

【発明の効果】以上述べたごとく、本発明によれば、コンピュータ設備とユーザの間の公衆交換電話網のモデム間の再認証手続きによって、侵入者によるアクティブ傍受に対してコンピュータ設備を保護する安全な方法が実現される。

【図面の簡単な説明】

【図１】二地点間データ通信システムのブロック図である。

【図２】図１のデータ通信システムで使用される本発明の原理を使用したモデムのブロック図である。

【図３】図２のモデムで使用される方法の流れ図である。

【図４】本発明の原理を使用する再認証手続きの流れ図である。

【図５】図２のモデムで使用されるもう１つの方法の流れ図である。

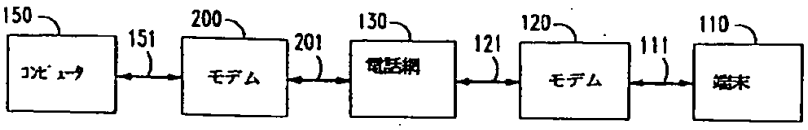
【図６】図２のモデムで使用される帯域外サイドチャネルの図である。

【図７】図２のモデムで使用される帯域内サイドチャネルの図である。

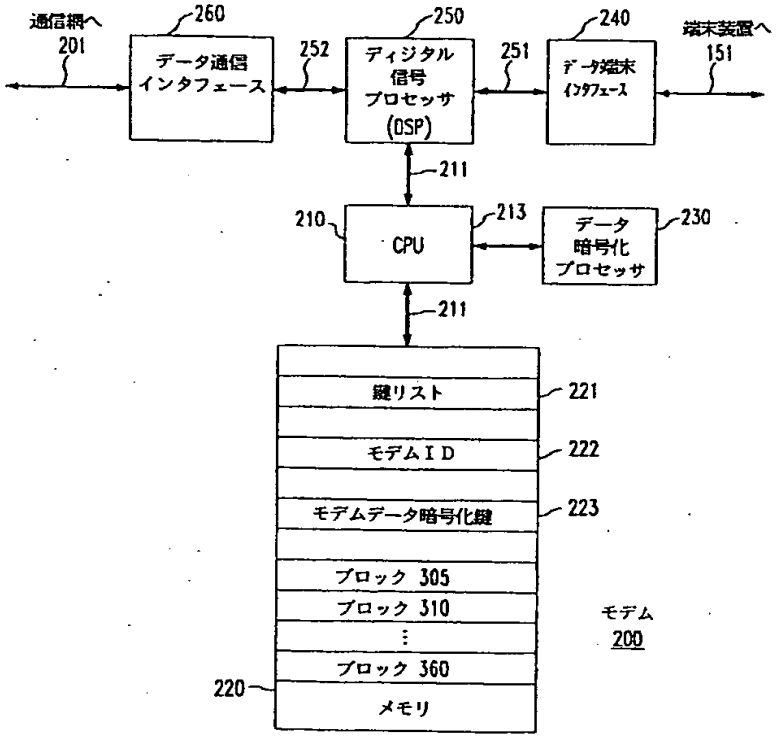
【符号の説明】

１１０　端末
１２０　発信モデム
１３０　電話網
１５０　コンピュータ
２００　着信モデム
２１０　ＣＰＵ
２２０　メモリ
２２１　鍵リスト
２３０　データ暗号化プロセッサ
２４０　データ端末インタフェース
２５０　ディジタル信号プロセッサ（ＤＳＰ）
２６０　データ通信インタフェース
４０５　補助（狭帯域）チャネル
４１０　基本チャネル
５０５　制御フレーム
５１０　データフレーム

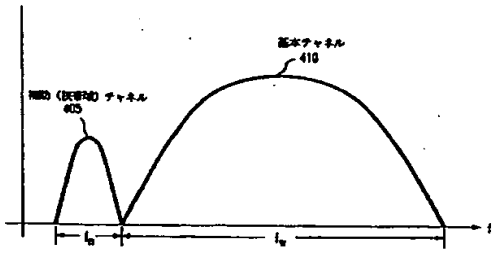
【図１】



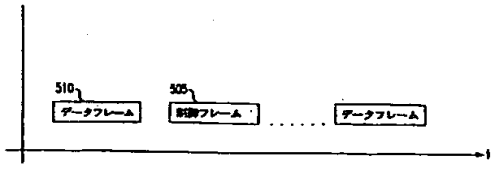
【図2】


通信網へ
201
260
データ通信
インタフェース
252
250
ディジタル
信号
プロセッサ
(DSP)
251
240
データ端末
インタフェース
端末装置へ
151
211
210
CPU
213
データ
暗号化
プロセッサ
230
211
鍵リスト
221
モデムＩＤ
222
モデムデータ暗号化鍵
223
ブロック 305
ブロック 310
ブロック 360
220
メモリ
モデム
200

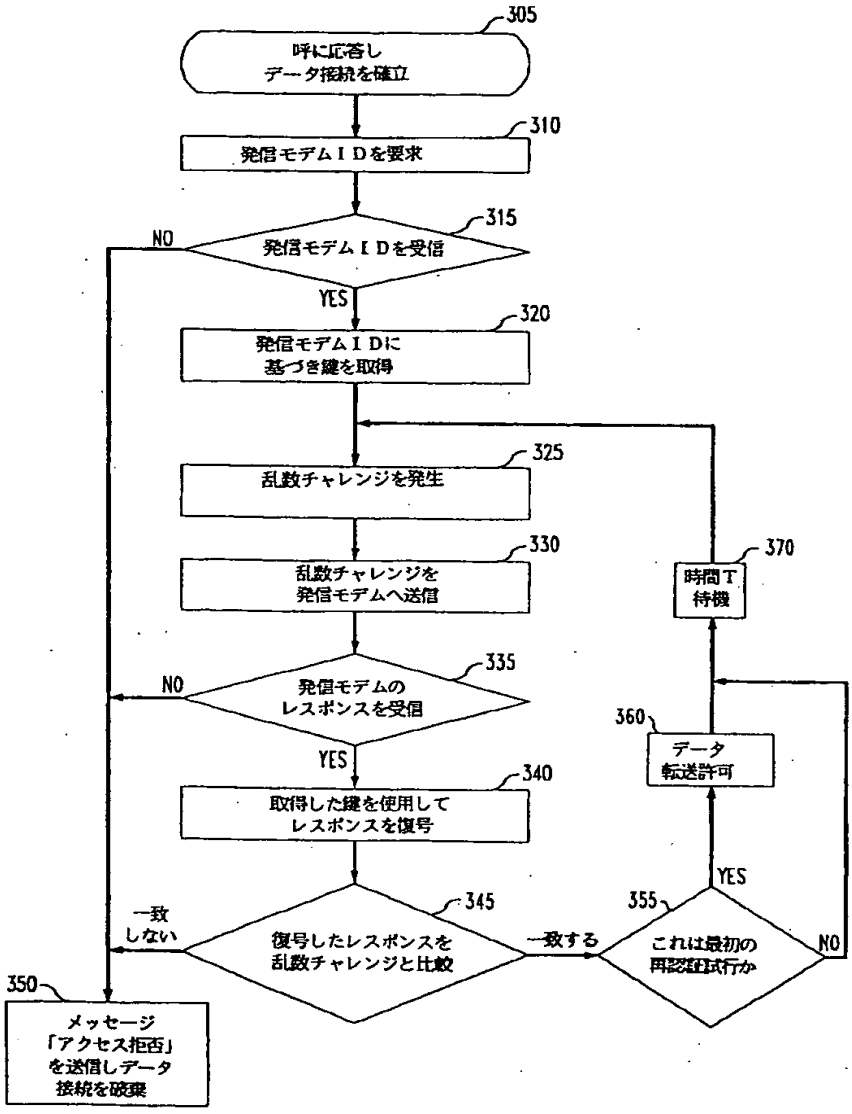
【図6】


基本チャネル
410
405
t

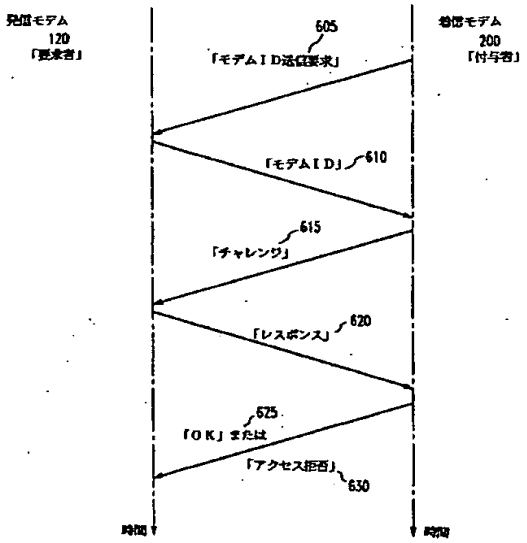
【図7】


510
データフレーム
505
データフレーム
t

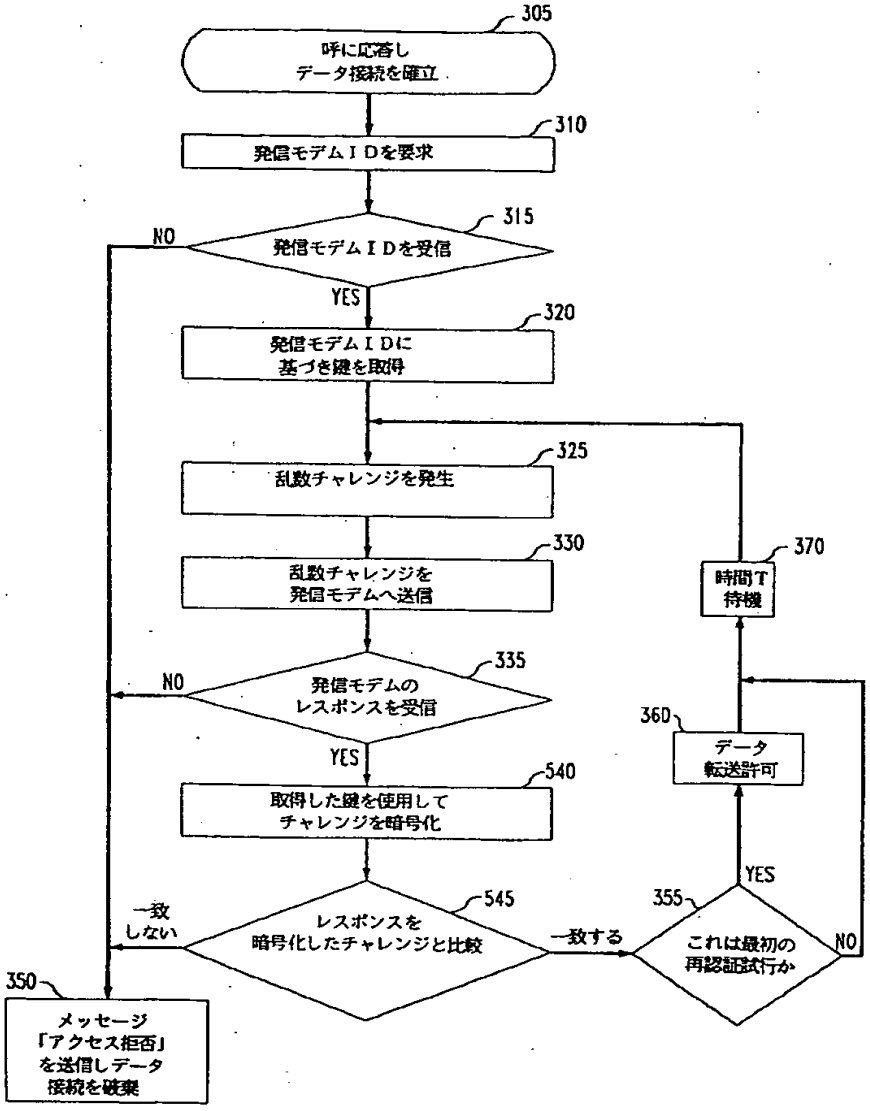
【図3】


305
呼に応答し
データ接続を確立
310
発信モデムＩＤを要求
315
NO
発信モデムＩＤを受信
YES
320
発信モデムＩＤに
基づき鍵を取得
325
乱数チャレンジを発生
330
乱数チャレンジを
発信モデムへ送信
335
NO
発信モデムの
レスポンスを受信
YES
340
取得した鍵を使用して
レスポンスを復号
345
一致
しない
復号したレスポンスを
乱数チャレンジと比較
一致する
350
メッセージ
「アクセス拒否」
を送信しデータ
接続を破棄
355
これは最初の
再認証試行か
YES
NO
360
データ
転送許可
370
時間Ｔ
待機

【図4】


発信モデム
120
「要求者」
着信モデム
200
「付与者」
605
「モデムＩＤ送信要求」
「モデムＩＤ」
610
615
「チャレンジ」
「レスポンス」
620
625
「ＯＫ」または
「アクセス拒否」
630
時間
時間

【図5】




フロントページの続き

| (51)Int.Cl.5 | 識別記号 | 庁内整理番号 | ＦＩ | 技術表示箇所 |
|---|---|---|---|---|
| Ｈ０４Ｌ　12/22 | | | | |
| Ｈ０４Ｍ　11/00 | ３０３ | 7470－5Ｋ | | |

(72)発明者 ロバート アール スコット
アメリカ合衆国 34630 フロリダ クリアウォーター、ナンバ204、ベイウェイブルヴァード 640

(72)発明者 リチャード ケント スミス
アメリカ合衆国 34646 フロリダ セミノール、アルパイン アヴェニュー 13471